US 20060095548A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2006/0095548 A1

Rabot et al. (43) Pub. Date: May 4, 2006

(54) METHOD FOR THE AUTOMATIC SELECTION OF A SECURITY CONFIGURATION FOR TERMINALS OF NOMAD USERS

(76) Inventors: **Wilfrid Rabot**, Cresserons (FR); **Ivan Lovric**, Lunel (FR); **Pierre Cazenave**, Eterville (FR)

Correspondence Address:
FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022 (US)

(21) Appl. No.: **11/241,017**

(22) Filed: **Sep. 30, 2005**

(30) **Foreign Application Priority Data**

Oct. 1, 2004 (FR) 0410400

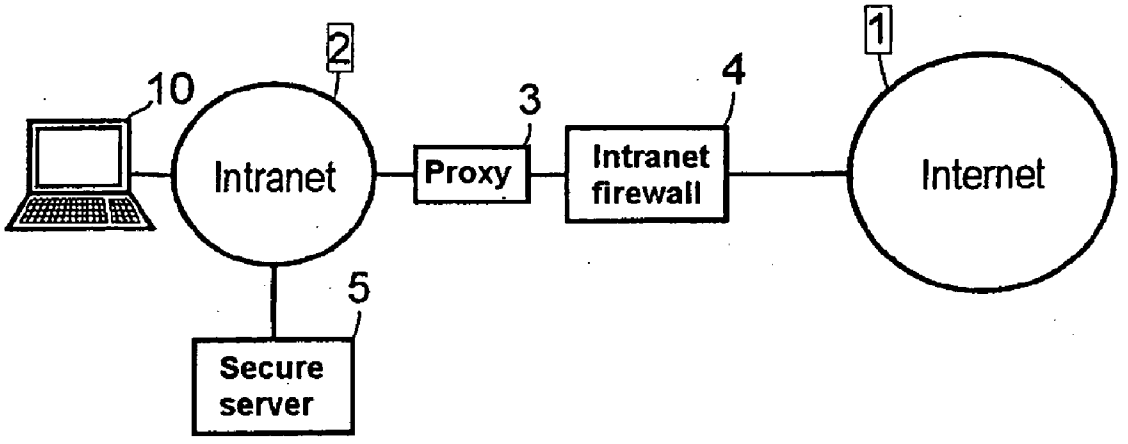
Publication Classification

(51) **Int. Cl.**
G06F 15/177 (2006.01)

(52) **U.S. Cl.** **709/220**

(57) **ABSTRACT**

Method for selecting a security configuration of a user's terminal (**10**) able to be connected to at least one network (**1, 2**) via several network interfaces, comprising steps during which the terminal (**10**): detects any change in the terminal's physical connection to a network; verifies that the terminal is connected to a network by a unique physical link; disconnects all physical links with a network so as to maintain only one physical link; determines the characteristics of the maintained physical link; and configures the terminal in relation to the characteristics of the maintained physical link.



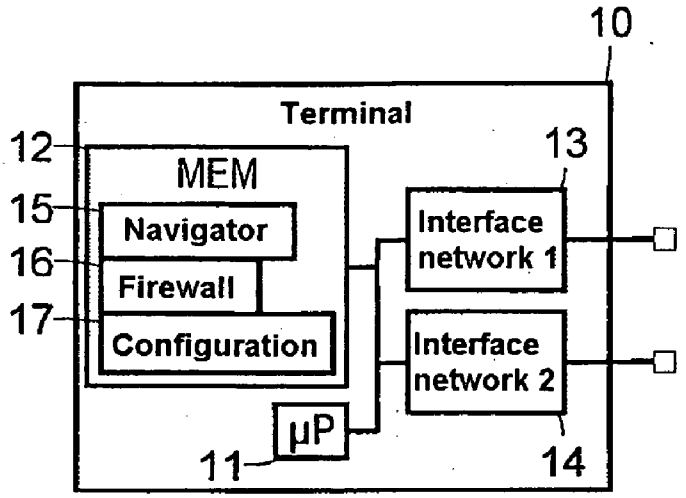


Fig. 1

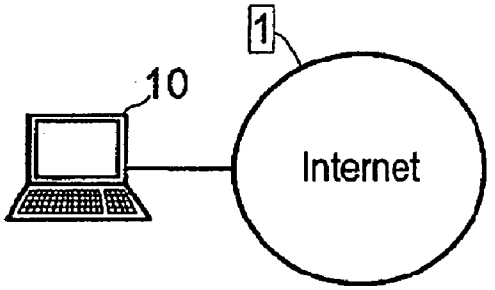


Fig. 2

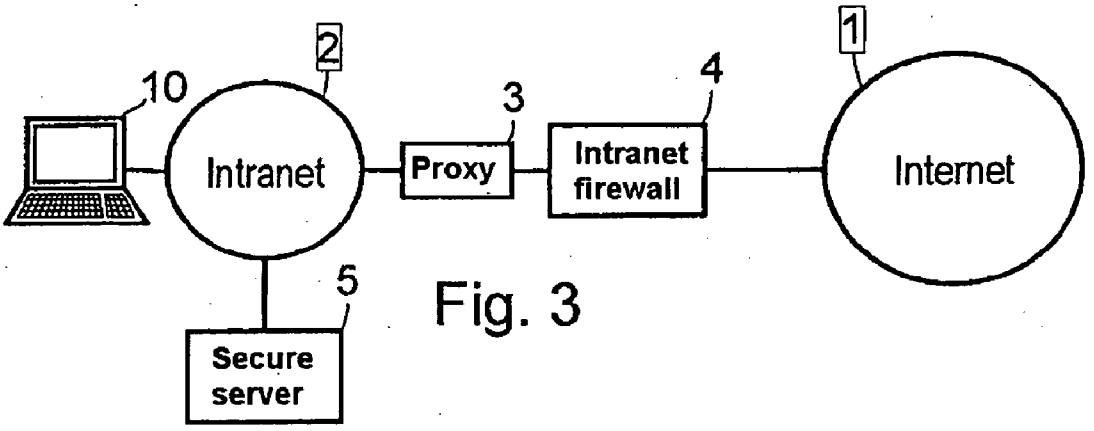


Fig. 3

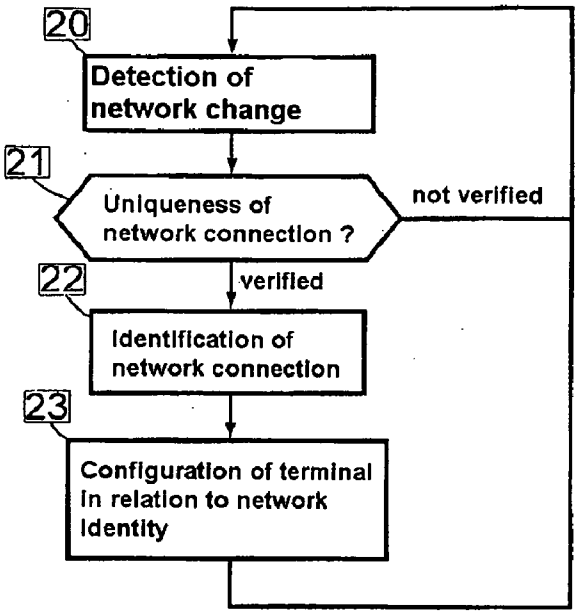

20
Detection of network change
21
Uniqueness of network connection ?
not verified
verified
22
Identification of network connection
23
Configuration of terminal in relation to network identity

Fig. 4

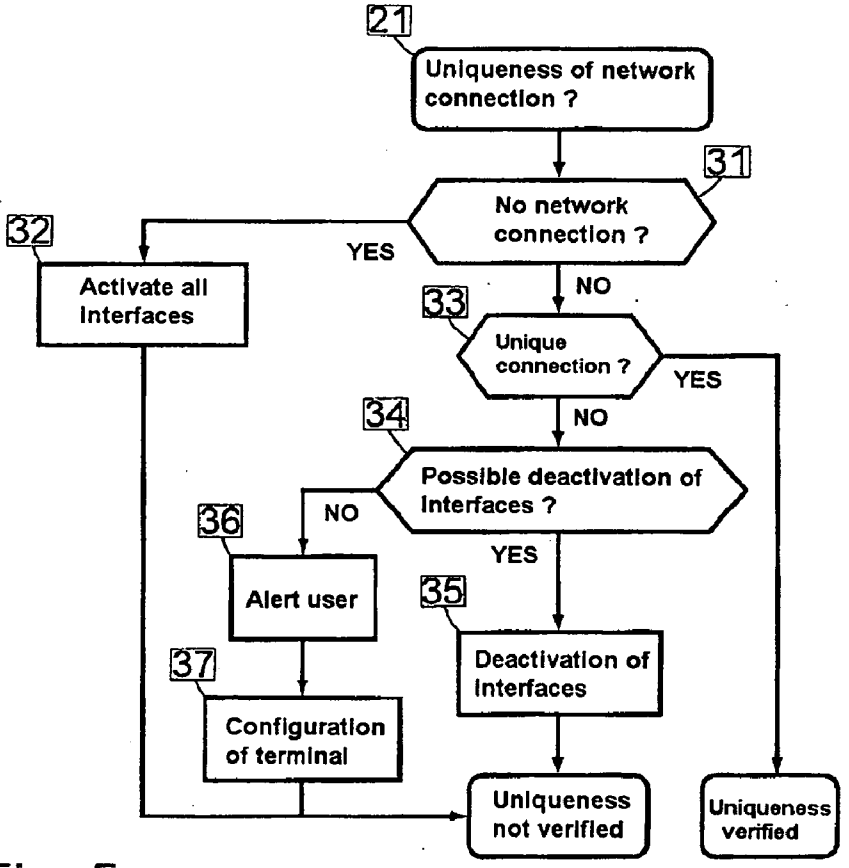

21
Uniqueness of network connection ?
31
No network connection ?
YES
32
Activate all Interfaces
NO
33
Unique connection ?
YES
NO
34
Possible deactivation of Interfaces ?
NO
36
Alert user
YES
35
Deactivation of Interfaces
37
Configuration of terminal
Uniqueness not verified
Uniqueness verified

Fig. 5

METHOD FOR THE AUTOMATIC SELECTION OF A SECURITY CONFIGURATION FOR TERMINALS OF NOMAD USERS

[0001] The present invention relates to the protection of terminals when they are connected to a private or public computer network, such as the Internet.

[0002] It applies particularly, but not exclusively, to terminals of nomad users, irrespective of the network to which they are connected, the connection mode and the type of terminal. Hence the network may be of Ethernet, WiFi, GPRS (General Packet Radio Service), ADSL (Asymmetric Digital Subscriber Line), PSTN (Public Switched Telephone Network) type, . . . , the connection mode may be of wire or wireless type (Bluetooth for example) with or without intermediate proxy, and the terminal may be of PC, PDA type, ...

[0003] At the current time, nomad users have increasingly more network connection means. With the development of wireless networks such as WiFi and Bluetooth, nomad user terminals generally have several network interfaces which may be activated simultaneously. In addition, some of these network interfaces may connect automatically, for example on start-up of the terminal with no particular action on the user's part. As a result the security of said terminals is affected.

[0004] To overcome this drawback, users must permanently and manually check the uniqueness of their network connection.

[0005] In general, the security of a terminal is ensured by what is called a firewall which in some situations, nomad situations in particular, must be configured manually by the user and activated or deactivated depending on whether or not the terminal is connected to a secure environment.

[0006] The most frequent case occurs with users having a laptop which they can use at their usual workplace or outside thereof. For this purpose, the laptop has an Ethernet network interface (wireline) or a WiFi interface with which to connect to a local network, the local network itself being connected to a public IP network such as the Internet via a proxy and a firewall. When users have nomad status (outside their usual workplace) they can connect to the Internet via the WiFi interface and firewall software installed in the laptop.

[0007] At the current time, whenever users leave their office and access the Internet under nomad status, or return to their office, they must manually configure their network interface cards, firewall and proxy parameters of their navigator. This leads to major risks of error which could have serious consequences if the security functions are not correctly activated or if the terminal is connected to the Internet simultaneously via a secure local network and a WiFi interface. Configuration errors may also prevent the terminal from connecting to the local network or Internet, or from being remotely updated (software and anti-virus updates) when connected to a secure local network. Such configuration errors may also involve dysfunction of the web browser (wrong configuration of proxy parameters) making Internet connections impossible and having the consequences of time losses and unnecessary calls to computer assistance services.

[0008] The situation becomes further complicated if the user's terminal has more than two network interfaces, each interface then being associated with a respective network environment and security configuration consisting of a set of configuration parameters, firewall parameters in particular.

[0009] The present invention sets out to overcome these drawbacks and in particular to securitize the terminal's network connection.

[0010] For this purpose, the invention proposes a method comprising steps during which the terminal:

[0011] verifies whether the terminal is connected to a network by a unique physical link,

[0012] if uniqueness of connection is not verified, disconnects all physical links with a network so as to maintain only one physical link,

[0013] determines the characteristics of the maintained physical link, and

[0014] configures the terminal in relation to the characteristics of the maintained physical link.

[0015] Advantageously, an order of priority is allocated to each of the possible physical links of the terminal with a network, the maintained physical link having highest priority.

[0016] According to a preferred embodiment of the invention, if a physical link with a network cannot be disconnected, the terminal emits an alert message to the user and configures the terminal taking active physical links into account.

[0017] According to a preferred embodiment of the invention, the determination of the characteristics of a physical link with a network comprises an identification step of a possible local network to which the active network interface is connected, by attempting connection to a secure server known to the terminal and supposedly visible solely to the local network.

[0018] According to a preferred embodiment of the invention, the configuration of the terminal consists of selecting a set of parameter values corresponding to the maintained network link.

[0019] According to a preferred embodiment of the invention, the step consisting of verifying whether the terminal is connected to the network via a unique link is preceded by a detection step to detect a change in physical connection of the terminal to a network.

[0020] According to one variant, the detection step is triggered periodically.

[0021] According to another variant, the detection step is triggered on receipt of a system event.

[0022] The invention also concerns an automatic configuration programme of the security of a terminal able to be connected to at least one network via several network interfaces, this programme comprising programme code instructions to carry out the above-defined method when the programme is executed on a terminal.

[0023] The invention also concerns a terminal containing said programme.

[0024] The invention also concerns a nomad user's terminal comprising at least two network interfaces to connect to

at least one network, a firewall and navigational software. According to the invention, this terminal comprises programmed processing means to:

[0025] verify that the terminal is connected to a network by a unique physical link,

[0026] if uniqueness of connection is not verified, disconnect all physical links with a network so as to maintain only one physical link,

[0027] determine the characteristics of the maintained physical link, and

[0028] configure the terminal in relation to the characteristics of the maintained physical link.

[0029] Advantageously, the processing means are programmed to allocate an order of priority to each of the possible network links of the terminal, the maintained network link being giving highest priority.

[0030] According to a preferred embodiment of the invention, the processing means are programmed to emit an alert message to the user if a physical link cannot be disconnected, and to configure the terminal taking several active physical links into consideration.

[0031] According to a preferred embodiment of the invention, the processing means are programmed to identify a possible local network to which the active network interface is connected, by conducting an attempted connection to a secure server known to the terminal and supposedly visible solely to the local network.

[0032] A preferred embodiment of the invention is described below as a non-restrictive example with reference to the appended drawings in which:

[0033] **FIG. 1** is a schematic of a nomad terminal;

[0034] **FIG. 2** is a schematic of the environment of the terminal shown in **FIG. 1**, connected to a public network;

[0035] **FIG. 3** is schematic of the environment of the terminal shown in **FIG. 1** when it is connected to the same public network via a private local network;

[0036] **FIG. 4** is a flow chart of the different steps of the method in accordance with the invention,

[0037] **FIG. 5**, in more detail in the form of a flow chart, shows one of the steps of the method illustrated **FIG. 4**.

[0038] **FIG. 1** shows a terminal **10** for example of laptop type or personal electronic assistant (PDA) type comprising several network interfaces **13**, **14** to connect in different ways to a network such as the Internet, a processor **11**, data and programme memories **12** memorising a web browser **15**, and a firewall **16** for protection against intruder attempts from the network.

[0039] The network interfaces **13**, **14** may be of Ethernet network card type, modem (ADSL, PSTN, GPRS), WiFi interface, Bluetooth interface, etc. These interfaces may also be of the same type. Therefore the terminal may for example comprise two WiFi interfaces and one PSTN modem.

[0040] With this configuration terminal **10** can for example be connected directly to a public network **1** such as the Internet as illustrated **FIG. 2**, or via a local network **2** as illustrated **FIG. 3**. Such connection can be either physical using a physical interface, or virtual to obtain an advanced service (virtual private network . . .) on one or more physical connections.

[0041] In **FIG. 3**, terminal **10** is connected to a private local network **2** such as a local company network or Intranet, this network itself being connected to the public network **1** via a proxy **3** and a firewall **4**. The connection between the terminal and the local network is conventionally made via an Ethernet interface.

[0042] Changing between the configurations illustrated **FIGS. 2 and 3** requires configuration of the network interfaces **13**, **14** installed in the terminal, of the firewall **16** and of the proxy parameters of the web brower **15**.

[0043] For this purpose, terminal **10** is equipped, according to the invention, with an automatic configuration device **17**, advantageously in the form of a programme designed to verify permanently that the terminal is connected to a network **1**, **2** by a unique physical link, to determine the type of network to which the terminal is so connected and to select a security configuration in relation to the network and the type of link with this network.

[0044] As illustrated **FIG. 4**, the configuration device **17** is designed to detect a change in physical connection to a network, and on each detection of said change to execute a procedure **20** comprising execution of a verification procedure **21** verifying that the terminal **10** is connected to a network **1** by a unique physical link. If uniqueness of the network connection is not verified, the device again executes procedure **20**. If not the device identifies the physical connection at the next step **22**, then at following step **23** configures the terminal in relation to the type of physical connection identified during the previous step.

[0045] Detection of a change in physical connection to a network consists of determining changes in the connected/disconnected status of the network interfaces of terminal **10**. This detection may be performed by verifying the connected/disconnected status of the network interfaces which can be triggered either periodically or on receipt of a system event (such as a change in IP address).

[0046] Verification of the uniqueness of the. terminal's physical connection to a network consists of verifying that a single physical connection is active on the terminal at a given time. This verification consists of applying the following rules:

[0047] if no physical connection is active, all the network interfaces are activated,

[0048] when two network interfaces are detected as being simultaneously connected, the device attempts to disable the network interfaces defined as having lower priority.

[0049] An example of procedure **21** for verifying uniqueness of the physical connection is illustrated **FIG. 5**. In this figure, during a first step **31** the procedure tests whether a network interface of the terminal is active. If no network interface is active, all the network interfaces are activated at step **32** and procedure **21** ends by feeding back that uniqueness of the network connection is not verified. If at step **31** at least one network interface is active, the procedure tests at step **33** whether several network interfaces are active. If only one network interface is active, procedure **21** ends by feeding back that uniqueness of the physical connection with a network is verified. If not, procedure **21** attempts at step **34** to disable the network interfaces having least priority so as only to maintain the one with the highest priority.

[0050] The order of priority of the physical connections may be chosen as follows:

[0051] 1. connection via a modem (STN, GPRS, ADSL),

[0052] 2. connection via an Ethernet wire link,

[0053] 3. connection via a WiFi link,

[0054] 4. connection via a Bluetooth link.

[0055] All these connections may be disable with the exception of the connections via modem. Therefore if the user sets up several connections with modems, the procedure alerts the user (step **36**) that several modems are simultaneously connected, and configures the terminal to ensure the greatest security (activation of the local firewall **16**) having regard to these connections (step **37**).

[0056] In the other cases, solely the physical connection having highest priority is maintained (step **35**). In particular, if terminal **10** is connected to the network via the WiFi interface, a physical connection via the Ethernet wire link causes disabling of the WiFi link. Procedure **21** then ends by feeding back that uniqueness of the physical connection is not verified.

[0057] Identification of the network connected to the physical interface (step **22**) is performed in securitized manner using authentication parameters for access to the network (**802**, **1**x, . . .) or by attempting connection to a server accessible solely in the local network using a secure protocol (SSL, HTTPS, . . .).

[0058] For example, as shown **FIG. 2**, an HTTPS server **5** visible only in the local network **2** may be used to identify this network: if the address of the server **5**, known to the terminal, effectively gives access to a server and if this access is secure (server authentication) then the terminal is indeed connected to the local network **2**.

[0059] The configuration of terminal **10** in relation to the network and/or network interface (step **23**) consists of selecting a security configuration (activation/configuration of a firewall, setting up a connection of virtual private network type . . .) and of configuring other applications non-related to security but depending upon the connected local network, such as the terminal's navigator (navigator's proxy parameter). The terminal therefore memorizes a configuration (set of values for security parameters and configuration) for each possible terminal link with the public network **1**.

1. Method of selecting a security configuration for a user's terminal able to be connected to at least one network by several network interfaces,

characterized in that it comprises steps during which the terminal;

verifies whether the terminal is connected to a network by a unique physical link,

if uniqueness of connection is not verified, disconnects all physical links with a network so as to maintain only one physical link,

determines the characteristics of the maintained physical link, and

configures the terminal in relation to the characteristics of the maintained physical link.

2. Method as in claim 1,

characterized in that an order of priority is allocated to each of the possible physical links of the terminal with a network, the maintained physical link having highest priority.

3. Method as in claim 1,

characterized in that if a physical link with a network cannot be disconnected, the terminal emits an alert message to the user and configures the terminal taking the active physical links into account.

4. Method as in claim 1,

characterized in that determination of the characteristics of a physical link with a network comprises an identification step of a possible local network to which the active network interface is connected, by attempting connection to a secure server known to the terminal and supposedly visible solely to the local network.

5. Method as in claim 1,

characterized in that the configuration of the terminal consists of selecting a set of parameter values corresponding to the maintained network link.

6. Method as in claim 1 wherein the step consisting of verifying whether the terminal is connected to the network via a unique link is preceded by a detection step to detect a change in physical connection of the terminal to a network.

7. Method as in claim 6, wherein the detection step is triggered periodically.

8. Method as in claim 1, wherein the detection step is triggered on receipt of a system event.

9. Automatic configuration program of the security of a terminal able to be connected to at least one network via several network interfaces characterized in that it comprises program code instructions to carry out the method as in claim 1 when the program is executed on a terminal.

10. Terminal comprising the program as in claim 9.

11. Nomad user's terminal comprising at least two network interfaces to connect to at least one network, a firewall and navigational software,

characterized in that it comprises processing means programmed to:

verify whether the terminal is connected to a network by a single physical link,

if uniqueness of connection is not verified, disconnect all physical links with a network so as to maintain only one physical link,

determine the characteristics of the maintained physical link, and

configure the terminal in relation to the characteristics of the maintained physical link.

12. Terminal as in claim 11,

characterized in that the processing means are programmed to allocate an order of priority to each of the possible network links of the terminal, the maintained network link having highest priority.

* * * * *